Adaptive Defense 360

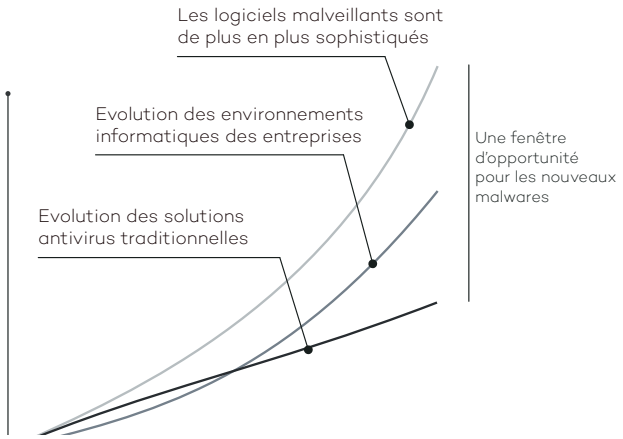
Find the answers, solve the problem

DÉFENSE INTÉGRALE POUR TERMINAUX ET SERVEURS INTÉGRANT PROTECTION, DÉTECTION, INTERVENTION ET RESTAURATION DANS UNE SOLUTION UNIQUE

La défense des postes de travail contre les cyber-attaques est une tâche difficile. Elle doit inclure une large variété d'outils de défense comprenant une protection antivirus/antimalware, un firewall personnel, du filtrage web et email et le contrôle des appareils connectés. En outre chaque protection doit aussi offrir des dispositifs de défense supplémentaires contre les attaques ciblées et zero-day. Jusqu'à présent, les directions informatiques avaient besoin d'acheter et maintenir des solutions émanant de différents fournisseurs pour protéger leurs terminaux.

Adaptive Defense 360 est la première offre à combiner les capacités d'une protection EPP (Endpoint Protection Platform) et d'une solution EDR (Endpoint Detection & Response) dans une solution unique.

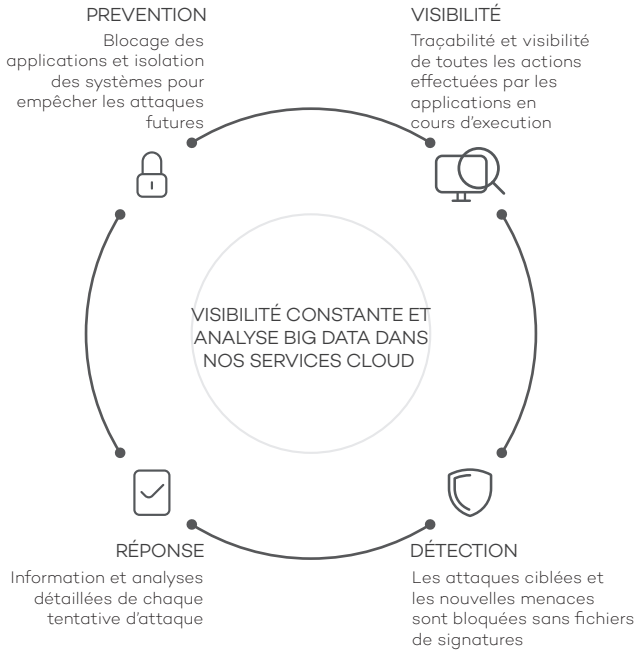
Adaptive Defense 360 intègre tout d'abord la protection EPP la plus complète de Panda, avec une surveillance et des rapports de sécurité en temps réel, des outils correctifs et curatifs, une protection par profil d'utilisateur, le contrôle centralisé des appareils mobiles connectés, la surveillance et le filtrage Web.



Mais ce n'est désormais plus suffisant. Le volume et la sophistication des logiciels malveillants et des outils de sécurité informatique ont beaucoup évolué. Avec plus de 200 000 nouveaux virus identifiés en moyenne chaque jour et la sophistication des techniques utilisées pour percer les défenses et dissimuler les codes malveillants, les réseaux d'entreprise sont plus vulnérables que jamais aux attaques ciblées ou de type zero-day.

Les solutions de protection traditionnelles sont efficaces pour neutraliser les malwares connus par le biais de techniques de détection basées sur des bases de signature et des algorithmes heuristiques. Cependant elles ne protègent pas contre les attaques ciblées et zero-day qui exploitent la "fenêtre d'opportunité des logiciels malveillants", c'est-à-dire le temps qui s'écoule entre l'apparition d'un nouveau virus et la publication de son antidote par les éditeurs de solutions de sécurité. Cette latence, de plus en plus longue, est exploitée par les pirates pour introduire des virus, des logiciels de rançon, des chevaux de Troie et d'autres types de logiciels malveillants dans les réseaux des entreprises. Ces menaces, qui se banalisent, peuvent aller du cryptage de documents confidentiels en échange d'une rançon au recueil de données sensibles à des fins d'espionnage industriel.

Adaptive Defense 360 a été developpé pour parer efficacement ce type d'attaques: La solution inclut un service EDR (Endpoint Detection & Response) capable de classifier avec précision chaque application qui s'exécute dans votre entreprise, en autorisant uniquement l'exécution des programmes identifiés comme légitimes. Les capacités EDR s'appuient sur un modèle de sécurité reposant sur trois principes : La surveillance constante des applications qui fonctionnent sur les ordinateurs et serveurs d'une entreprise, la classification automatique par un apprentissage machine exploitant notre plate-forme Big Data sur le Cloud, et enfin, l'analyse par nos experts techniques des applications n'ayant pas été classifiées automatiquement afin de déterminer avec certitude le comportement de tout ce qui s'exécute sur les systèmes de l'entreprise.



LA SEULE SOLUTION POUR GARANTIR LA SÉCURITÉ DE TOUTES LES APPLICATIONS EN FONCTIONNEMENT

GARANTIE D'UNE PROTECTION FIABLE ET COMPLÈTE

Panda Adaptive Defense 360 offre deux modes d'action :

• **Le mode standard** autorise, après une phase d'audit, l'exécution de toutes les applications cataloguées comme inoffensives ainsi que les systèmes automatisés. Les processus inconnus ou en provenance de l'exterieur sont bloqués par défaut jusqu'à la fin de leur classification.

• **Le mode étendu** permet uniquement l'exécution des logiciels catalogués inoffensifs apres une longue phase d'apprentissage. Il est recommandé aux organisations qui souhaitent une approche 'à risque zéro' de la sécurité.

RÉSULTATS D'ANALYSE A POSTERIORI

• Les **graphiques des événements d'exécution** donnent une vue claire de tous les événements provoqués par des logiciels malveillants.

• Bénéficiez, grâce aux **cartes de températures,** d'informations visuelles sur la source géographique des connexions de logiciels malveillants, des fichiers créés, etc.

• Localisez les logiciels installés sur votre réseau et comportant des vulnérabilités connues.

PROTECTION POUR LES SYSTÈMES D'EXPLOITATION ET LES APPLICATIONS VULNÉRABLES

Les systèmes tels que Windows XP, qui ne sont plus supportés par leur éditeur, ne reçoivent plus de correctifs et sont donc vulnérables ; ils deviennent des proies faciles pour les menaces nouvelles (zero-days) et les attaques de nouvelle génération.

En outre, les vulnérabilités dans les applications comme Java, Adobe, Microsoft Office et les navigateurs sont exploitées par 90 % des logiciels malveillants.

Le module de protection contre les vulnérabilités d' **Adaptive Defense 360** utilise des règles contextuelles et comportementales pour permettre aux entreprises de travailler dans un environnement sécurisé même avec des systèmes qui n'ont pas été mis à jour.

TOUTES LES CAPACITÉS D'UNE SOLUTION EPP

Adaptive Defense 360 intègre Panda Endpoint Protection Plus, la solution EPP (Endpoint Protection Platform) la plus avancée de Panda, qui inclue notamment :

- Actions correctives et curatives en cas d'infection
- Contrôle centralisé des terminaux : Prévient infections et pertes de donnée par un blocage par type d'appareil
- Surveillance et filtrage Web
- Protection antivirus et anti-spam pour serveur Exchange
- Firewall pour les terminaux, personnel ou administré...

INFORMATIONS EN TEMPS RÉEL SUR L'ÉTAT DU RÉSEAU

Bénéficiez d'alertes immédiates dès qu'un logiciel malveillant est identifié dans le réseau, avec un rapport complet détaillant l'emplacement, les ordinateurs infectés et l'action entreprise par le logiciel malveillant.

Recevez des rapports par e-mail sur l'activité journalière du service.

ACCESSIBLE AUX SYSTÈMES SIEM

Adaptive Defense 360 s'intègre à des solutions SIEM pour fournir des informations détaillées sur l'activité de toutes les applications qui s'exécutent sur vos systèmes.

Pour les clients sans SIEM, **Adaptive Defense 360** inclut son propre système de stockage et de gestion des événements de sécurité afin d'analyser toutes les informations. collectées en temps réel.

SERVICE GÉRÉ À 100%

Vous n'aurez plus à investir dans du personnel technique pour traiter les fichiers suspects ou placés en quarantaine ou bien pour désinfecter et restaurer les ordinateurs infectés. **Adaptive Defense 360** classifie automatiquement toutes les applications grâce à son apprentissage machine dans nos environnements Big Data sous la supervision constante des experts de PandaLabs.

CONFIGURATION MINIMALE REQUISE

Console Web (surveillance uniquement)

- Connexion Internet
- Internet Explorer 7.0 ou ultérieur
- Firefox 3.0 ou ultérieur
- Google Chrome 2.0 ou ultérieur

Agent

- Systèmes d'exploitation (postes de travail) : Windows XP SP2 et ultérieur, Vista, Windows 7, 8 & 8.1
- Systèmes d'exploitation (serveurs): Windows 2003 Server, Windows 2008, Windows Server 2012
- Connexion Internet (directe ou via proxy)

Partiellement pris en charge (EPP uniquement):

- Linux, MAC OS X et Android